图书情报工作
第66卷 第5期 2022年3月

网络信息内容生态安全风险整体智治的理论框架与实现策略研究*

■ 周毅　张雪
苏州大学社会学院　苏州 215123　苏州大学数据治理与产业发展研究中心　苏州 215123

摘　要：[目的/意义]网络信息内容生态安全风险是一种全新的信息生态安全问题，从多个维度影响和威胁着总体国家安全。[方法/过程]以整体性治理、智慧性治理理论为基础，以技术中介理论为依据，提出网络信息内容生态安全风险整体智治的理论框架构建理念、逻辑关系和基本内容，具体阐释整体智治理论框架构建的意义。[结果/结论]研究表明，网络信息内容生态安全风险整体智治的理论框架是以信息技术为中介的整体性与智慧性治理的有机融合。为了具体推进其组织实施，可以从建设制度化的机制保障体系、实施智能化的技术支撑体系等方面进行实施路径的选择。

关键词：网络信息内容生态安全风险　整体智治　理论框架　实现路径
分类号：G203
DOI：10.13266/j.issn.0252－3116.2022.05.005

1　研究进展与问题提出

1.1　研究进展分析

目前，国内外学者对于网络信息内容安全风险的研究主要包括网络内容安全风险内涵与表现、内容安全风险治理内涵与治理模式阐释等方面。早期网络信息内容安全主要是指受到网络系统漏洞导致内容泄漏、网络间谍、网络垃圾信息等，强调信息内容的隐秘性、完整性和可用性等安全属性[1]。现在的网络信息内容安全主要是指泄露数据内容本身、生产或传播网络违规或不良信息等[2]。在不同时期或阶段，网络信息内容安全风险表现也各有侧重：①传统的网络信息内容安全风险主要涉及信息系统、网络结构和网络内容本身等要素的安全性。②目前网络内容安全风险正逐渐向隐私权风险、国家话语权与意识形态安全风险、内容低俗化风险、内容操纵风险、知识产权风险等为代表的内容风险综合体发展[3]。上述不同类型的网络信息内容安全风险会产生不同影响，例如，隐私权风险和知识产权风险等主要威胁公共利益和公民合法权益[4]；信息内容操纵风险主要危害国家与社会安全；话语权风险和意识形态风险主要危害国家公信力与国家政治安全[5]；内容低俗化风险主要影响社会主义核心价值观和网络文明建设[6]；网络记忆消失风险主要威胁国家记忆与文化传承安全等[7]。

目前学界和业界已经深刻认识到了上述不同类型网络信息内容安全风险的可能影响和潜在危害，并对其治理要素与治理模式等开展了初步研究。学界认识到网络信息内容安全风险治理的主旨是保障网络信息内容不被滥用，不良信息内容流动得到控制，涉及网络内容分级、过滤、删除等防控措施和内容监控预警与隐私保护等[8]。有学者认为网络信息内容安全风险治理主体主要由政府、企业、社会组织和公民等构成，它们在网络内容安全与网络空间治理中有着不同的地位、作用，主要运用法律政策、自律公约、技术工具等开展治理行为实践，在不同治理参与主体之间可以形成一定的互动关系，并产生一定的治理效果[9－10]。关于网络信息内容安全风险治理的客体对象研究，则主要聚焦在用户生成内容的质量[11－12]、突发事件与网络舆情安全[13]、网络空间安全[14－15]、网络侵权与信息安全[16]、数据开放安全[17]、网络负面信息治理[18]等诸多方面。围绕着网络信息内容安全风险治理工具或治理模式，国内外学者多从政策与法规、行业规范与信息伦

* 本文系国家社会科学基金一般项目"网络信息内容生态安全风险治理模式构建与实现研究"（项目编号：21BTQ013）研究成果之一。
作者简介：周毅，教授，博士生导师，E-mail：zhouy@suda.edu.cn；张雪，硕士研究生。
收稿日期：2021－06－06　修回日期：2021－11－01　本文起止页码：44－52　本文责任编辑：徐健

理、技术手段与工具等角度进行分析[19-20],初步形成了政府监管模式[21-22]、多元共治模式[9,23]和网络自治模式[24]3种典型模式。

综合而言,学界在该研究领域初步揭示了网络信息内容安全风险要素、产生原因、表现类型等,但阐释仍然比较零散,一般是以对负面信息内容的监管为主要治理对象并形成治理方法,没有明确提出并界定网络信息内容生态安全的内涵,没有对网络信息内容生态安全风险进行细粒度解析、演化趋势刻画和整体性治理实践。虽然认识到网络信息内容生态安全风险治理是多主体的行为,在理论上也提出了几种不同治理模式,但在运作上仍是针对特定专题内容或网络信息服务平台,以采取分散性、临时性、粗放式的运动式治理为主,治理行动的临时性与分散性特征比较明显,智慧性的精准治理还有很大提升空间。

1.2 问题提出

在Web2.0下用户生成内容(User generated content,UGC)已经成为一种网络信息内容生产的常态,用户行为的多样性和生成内容动机的复杂性使网络信息内容生态安全风险有增大趋势[25],各种违规或不良信息内容的流动与传播,从政治、文化、经济等维度对总体国家安全产生着重要影响。针对总体国家安全和网络治理体系与治理能力现代化的要求,结合UGC的内容组织与传播特点和《网络信息内容生态治理规定》《互联网信息服务管理办法》(修订稿)等政策动态,实现从网络不良信息内容监管向网络信息内容生态安全风险治理的转型,研究其治理模式的转型或构建就成为一个重要理论与实践问题。

网络信息内容生态安全风险是指由隐私权风险、国家话语权与意识形态安全风险、内容低俗化风险、内容操纵风险、知识产权风险和记忆消失风险等构成的内容安全风险综合体,它呈现出内容安全风险的相关性、动态性、多样性等特点,并以"内容聚集样态"的整体性面貌决定着网络信息内容生态安全风险的总体态势。本文采用文献研究法和比较研究法,以"网络信息内容生态安全风险"为研究对象,以整体性治理、智慧性治理理论为基础,发挥技术中介理论的联接作用,提出一个整体智治的理论框架,从而实现从目前的负面信息防控监管到以"内容聚集样态"为中心的治理、从单一的网络信息内容安全风险表现管控到网络信息内容生态安全风险整体性治理的转变,旨在营造一个良性循环的网络信息内容生态安全环境。

2 网络信息内容生态安全风险整体智治的理论框架

2.1 网络信息内容生态安全风险治理及其构成要素

网络信息内容生态安全风险治理是指以政府为主导的多元主体通过运用大数据技术、人工智能技术等,以网络信息内容生态安全风险为治理对象,按照一定的规则体系推动多元主体的有效协调,实现网络信息内容生态安全风险的精准、高效、有序治理,从而构建一个良好的网络信息内容生态安全环境。在上述概念中所包含的治理构成要素主要包括:

2.1.1 治理主体要素

网络信息内容生态安全风险治理包括各类利益相关的行动者[26],即网络信息内容生态安全风险治理行动场域中的所有参与者,主要包括作为管理者的各级党委、政府及其网信管理部门、互联网行业组织等,既是治理主体又是治理相对人的网络信息服务平台(如作为内容生产者的ICP,作为传播服者的ISP),作为内容生产者、传播者和使用者的用户等等。在上述主体中,网络信息服务平台既是治理主体又是治理相对人,在不同治理场景下其身份角色会发生转换。

2.1.2 治理客体要素

网络信息内容生态安全风险治理指向的治理对象是网络信息内容生态安全。从理论上看,网络信息内容治理有两个不同的指向对象,即不良信息内容的监管和信息内容生态安全。指向不良信息内容的治理强调国家对网络信息内容质量的管控,指向信息内容生态安全的治理则强调将正负面信息内容均作为治理对象,并在两者的对向标示治理中保持内容聚集整体样态良好。从逻辑上看,网络信息内容生态安全风险治理是以"内容聚集样态"为中心,它不仅有针对不良信息内容的监管,而且也有正面信息内容的生产投放,是一种正负面信息内容的对向标示治理;它不仅关注信息内容的"量"或"质",而且关注多样态的网络信息内容聚集样貌[2]。因此,从治理对象的指向上看,现实的治理对象应该更加突出网络信息内容生态安全风险的整体性和系统性治理。

2.1.3 治理的工具与技术要素

工具与技术要素既包括行政管理手段及其相关工具,也包括技术手段与工具。从发展看,技术工具要素正逐步成为网络信息内容生态安全风险治理的关键核心要素。大数据技术、信息识别与过滤技术、信息集成

处理技术、智能服务技术等都是网络信息内容生态安全风险治理的核心保障。

2.1.4 治理的规则制度

规则制度包括网络安全法律法规、网络空间与社区管理组织结构[27]、网络信息服务平台内容管理流程、网络信息服务行业规范等，这些规则体系可以粗略分为制度性规则、技术性规则等类型。制度性规则主要包括法律法规（如《网络安全法》《互联网信息服务管理办法》等）和相关网络政策（如虚拟社区政策、网络市场政策、网事调节政策等）；技术性规则可以从两个层面进行理解。从实施治理的技术性操作过程看，整体性治理需要建立"多方联动、立体共责"的规则体系；从实施治理所应用的信息技术要求看，对有关主体在信息技术应用中的技术共享、技术安全等应建立标准规则。

2.1.5 治理的过程机制

治理就是要在内容生态安全风险场景要素解构基础上，实现对网络信息内容生态安全风险治理体系的构建[28]。所谓内容生态安全风险场景要素解构，就是要从风险类型、内容聚类、价值指向、传播节点等方面对网络信息内容生态安全风险现状和演化趋势等进行整体性刻画，认识风险类型与风险责任来源、风险后果之间的关系以及风险类型与风险识别方式、风险治理部门之间的关系。所谓内容生态安全风险治理体系构建是要构建一个多方联动、智能驱动、立体共责的网络信息内容治理机制[29]。多方联动是指要有效整合党委、政府、企业、社会力量等所有力量，形成党委领导、政府管理、企业履责、社会监督、网民自律等多主体协同的治理机制；智能驱动是指在发挥人工审查机制作用基础上，要充分发挥大数据技术、人工智能技术等的作用，根据网络信息内容产品形态来灵活定制不同的内容安全风险审查策略；立体共责是指通过权责边界的明确，对主体间的功能关系进行规范化的边界划分，建立起不同主体的权力与责任体系，从而提升网络信息内容生态安全风险的治理能力。

由上述要素所构成的网络信息内容生态安全风险治理模式会因组合结构方式、运行组织机制、制度规则体系和治理侧重点不同而形成不同的治理模式。正如前文所归纳发现的，目前国内外针对网络空间治理和网络信息内容安全治理已经形成了政府监管模式、多元共治模式和网络自治模式 3 种典型模式。上述 3 种模式在我国网络信息内容生态安全风险治理实践行动中已经取得了明显成效，但目前研究仍是针对特定专题或网络信息服务平台，以采取分散性、临时性、粗放式的运动式治理为主，部分内容服务平台的内部生态治理也表现出明显的自组织特点。如何以上述治理构成要素为基本条件，从理论框架上构建起一个有高度组织性的、针对生态整体样貌的、常态化的、精细化的内容生态安全治理体系就成为提高网络治理体系与治理能力现代化的关键。

2.2 网络信息内容生态安全风险整体智治的理论框架模型

20 世纪 90 年代，英国学者安德鲁 · 邓西尔（A. Dunsire）提出了"整体性治理"的概念，佩里 · 希克斯（P. Hicks）后又进一步提出了"整体性治理理论"[30]。整体性治理的核心内涵在于协调和整合，要在政府部门与市场部门、社会组织或私人实体之间达成共识和相互合作，它是一种治理主体多元、协作、耦合的全新治理模式。智慧性治理是在"技治主义"浪潮中提出的新型治理模式。智慧治理的逻辑从属于技术治理的逻辑，并形成了技术驱动、制度确认以及观念支持三维基础[31]。从上述理论表述看，整体性治理与智慧性治理存在着密切的内在联系，两者之间可以实现有机融合而不是简单相加。本文以整体性治理、智慧性治理理论为基础，以技术中介理论为联接，运用信息技术来消除和打破条线分割的主体界限，弥补资源碎片化、价值碎片化、部门碎片化、对象碎片化等缺陷，从而建构一个网络信息内容生态安全风险整体智治的理论框架。该理论框架是指通过广泛运用数字技术、人工智能技术等，推动治理主体之间的有效协调，实现整体性、系统性、精准性和智慧化的治理。如图 1 所示：

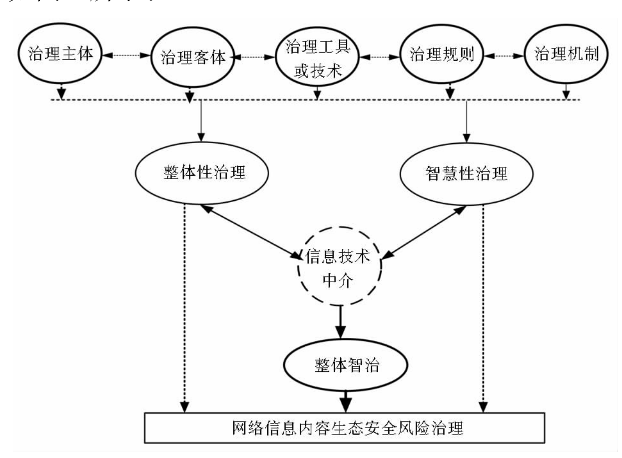


图 1 网络信息内容生态安全风险整体智治的理论框架

在上述整体智治理论框架的构建中，其主要构建逻辑和路线是：

2.2.1 实现整体性与智慧性融合的治理逻辑

在网络信息内容生态安全风险整体智治的理论框架构建中，应特别关注整理性治理和智慧性治理的治理主体、治理对象、治理工具、治理过程及治理规则等构成要素的组合方式，从而形成整体性和智慧性的融合治理逻辑。这种融合治理逻辑是以信息技术为中介来实现的，它推动多元主体的协调联动，促进正负面信息的对向标示治理，促进内容生态安全风险治理机制的运行流畅，最终实现网络生态风清气正和网络空间清朗的治理目标。对上述融合治理的逻辑解析，可以从治理主体、治理对象、治理机制和治理结果等构成要素的融合过程进行分析。

（1）治理主体视角。整体智治主要面对的是治理主体边界不清、权责不清、协同不力等问题。整体智治理论框架构建的主要理念和思路是厘清权责主体、划清治理边界、形成治理合力。其具体成效是各类不同主体的权责清单细化并形成较完备的主体分工、合作和协同机制体系。从目前看，随着政府有关部门将其网络内容监管权力向网络信息服务平台的转移，网络信息服务平台既是治理主体又是治理相对人，这就使其行动不可避免地会在应然责任与实然行动之间相互摇摆，网络信息服务平台的逐利性本质在一定程度上也使内容生态安全监管风险进一步加大。因此，如何给网络信息服务平台确权是一种对治理者的治理，实施详细的权力清单与责任清单制度应是构建不同治理主体协同配合机制的关键。

（2）治理对象视角。整体智治主要面对的是不良或违规信息内容泛滥和正能量信息内容生产与投放不足等问题。整体智治理论框架构建的主要理念和思路是运用多种手段获得并处理对象信息内容，主要包括对违规或不良信息内容的人工和智能识别、过滤与清除，对正能量信息内容的主动生产和投放等，促进治理对象指向从“不良内容”监管到“内容生态”整体样貌的变化，从个别或局部的网络信息内容服务平台治理到网络空间生态安全整体性治理的变化。治理对象的整体性强调对网络信息内容生态安全风险进行全景式观察，将网络信息内容生态安全风险表现及其相互关系作为一个系统来对待，而不是简单地将某类内容安全风险、某类信息服务平台、某类内容安全专题等作为治理对象，应实现从“个案”的选择性治理到“内容聚集样貌”的整体性治理转变。

（3）治理机制视角。整体智治与既有治理模式的主要区别在于，摒弃治理流程单一、治理对象指向单一、治理发动过程的临时性与碎片化以及主要依靠人工进行内容审查与事后删除等问题。整体智治理论框架构建的主要理念和思路是设计智能化、全景式、常态化、全程型的内容生态安全治理机制。这不仅仅限于风险应对，还应包括确立风险背景、识别风险性质、评估风险要素等环节，在风险面前取得主导权和控制权，这是一个动态性的治理过程[32]。从理想状态看，治理主体应能够根据内容生态安全风险生成的逻辑，思考如何吸收风险因素对网络内容生态所造成的扰动，并且使之恢复到原来的状态。同时，也会以此为契机对现状进行反思，深入探究网络内容生态安全风险事件和危机事件背后的根本原因。

（4）治理结果视角。整体智治主要面对的是内容生态安全风险治理结果的偶然性、安全风险时有发生的可能性和因治理所可能导致的用户体验变化等问题。由于网络不良或违规信息内容具有覆盖场景多、数据变种多、对抗性强、隐蔽性强等特点，这就使整体智治理论框架构建的主要思路应是聚焦于如何运用技术手段打破社会所框定的部门、区域、行业等主体在内容生态安全治理上的“边界”局限，打破不同网络信息服务平台的个体治理局限。整体智治所追求的开放性和包容性可以将具体的内容生态安全风险问题置于网络社区和社会关系的交错重叠之上，注重内容生态安全治理的整体效果，而非单一内容安全风险问题或风险事件的调处结果。其具体成效是网络内容生态安全风险识别精准、整体治理流程清晰、内容流动顺畅和用户体验良好。

2.2.2 发挥信息技术的中介和联接作用

技术现象学研究表明，技术在使用时常常“协助”塑造其实现功能的背景，技术会塑造人们的行为（actions）和认知（perceptions），并构建出新的实践和生活方式。现象学将这种现象称为“技术中介（technological mediation）”[33]。在网络信息内容生态安全风险治理中，高度发达的信息技术能够及时对复杂、冗繁的信息做出反应，便于治理主体之间的信息互动，从而在一定程度上有利于搭建起关系主体的关联性，可以助力并实现不同治理主体之间的联动（纵向科层化层级关系的整合、横向主体之间关系的协调）、不同内容生态安全风险要素的关联识别和不同治理流程的协同，形成“网络化”“多中心”“一体化”的治理格局，实现网络空间公共利益与网络信息服务平台利益、用户个人体验等之间的动态平衡，从而表征出对于网络内容异质性空间的包容和统合。

在整体智治的理论框架构建中，现代信息技术的中介和联接作用也有其内在的技术逻辑和特定场景：

（1）现代信息技术可以创建识别和分析内容生态安全风险及其安全整体状态的全新方式。通过实时性的内容敏感词汇识别，可以对内容生态安全风险进行细粒度分析，用数据及其关联性刻画出网络信息内容生态安全风险的真实情景和演变趋势，从而实现对不同类型或维度的网络信息内容生态安全风险治理的高效组织。

（2）现代信息技术可以创建网络信息内容自动审查与过滤的全新形式。例如，近年来已有多种内容智能审核系统正在被推广应用，这类系统的核心部分是由敏感词检测、人工干预操作、敏感信息替换以及分值效果回馈子系统组成，采用搜索技术将内容中涉及的敏感词查询出来，并且可以自动替换，还包含人工干预（修改误判、漏判）的成分，从而确保网络信息内容识别的有效性和准确性。这不仅可以极大地提高内容审查效率，而且在此基础上所采用的人工辅助判断也进一步提高了内容安全风险审查的可靠性和精准度。

（3）现代信息技术可以创建有关网络信息内容产品的自动化生产方式。有关研究表明，通过深入分析、挖掘和利用海量数据，围绕特定主题通过机器进行新闻内容的自动化生产已经成为一种可能。例如，腾讯公司的 DreamWriter，就可以根据算法在第一时间自动生成稿件，瞬时输出分析和研判，一分钟内将重要资讯和解读送达用户[34]。这种内容产品的自动化生产形式可以极大提高网络空间中正能量信息内容产品的生产与投放强度。

（4）现代信息技术可以创建网络内容生态安全风险治理状态评估的全新方式。例如，各类网络信息服务平台也可以利用大数据平台的海量数据及其计算优势，对各类不同用户进行精准画像，分析和刻画不同用户的内容生成兴趣与特点，及时发现不良或违规信息内容的来源及其风险，从而更好地对用户生产内容的趋势及其治理需求进行技术"验算"，确定内容生态安全风险治理的轻重缓急，合理进行平台内部的资源配置。

2.2.3 追求治理效率与价值的双重目标

整体智治强调内容生态安全风险治理的效率，即既要考虑治理行为的合理性与合法性，也考虑治理过程的高效性和协同性。整体智治的理论框架就是要运用现代信息技术来解决部门之间、层级之间、平台之间、功能之间、群体之间在网络信息内容生产、分发和传播过程中因价值差异、利益差异、规则差异等而导致的冲突和秩序混乱，通过技治、法治、德治等的融合，将网络信息服务平台异质性空间所呈现的分散化治理目标整合成为网络信息内容生态安全治理目标，从战略上回应总体国家安全的需要。从理论框架构建的逻辑上看，因信息技术的中介联接功能，可以使所有参与主体能够以"一个协同主体"的姿态或集体行动的逻辑对内容安全风险进行全方位、全天候的识别与分析，这可以部分替代对单一治理主体的能力要求[27]。在有关治理工具或方案研发中，由政府有关部门组织网络信息内容服务平台的技术力量共同研制内容特征信息库、开发通用的内容审查或过滤系统就成为技术审查能否实现的关键[35]。已有实践表明，上述设想目前可以不同程度地得到实现，这在一定程度上可以提升网络信息内容生态安全风险治理的有效性。

整体智治理论框架所追求的公共价值体现在总体国家安全和网络用户参与体验两个不同层面：①从宏观上看，内容生态安全风险整体智治所追求的公共价值目标是指要从内容生态安全风险的各种不同表现类型入手，通过识别、检索、过滤、删除、生产、投放等具体网络内容治理过程，从而构建一个集政治安全、文化安全、信息安全等于一体的安全动态集合体，就是要全方位地实现总体国家安全的公共价值目标。②从微观上看，用户的网络参与行为都有其一定的具体动机或目标追求，如休闲娱乐、政治参与、宣传展示、评论建议、经济利益等。经过多年的互联网实践和观点辩争，政学两界在互联网治理上已达成共识，即遵循法治原则，实行有限自由。用户既有利用网络公共空间进行意思表达的权利，但其也要在法律规定的范围内参与网络活动[36]。整体智治追求的公共价值在微观上就体现为寻求平衡网络信息服务平台和用户主体等的利益最大公约数，既使平台获得利益目标，也使用户获得良好的交流体验[37]。

整体智治理论框架的构建逻辑和路线，可以充分体现出网络信息内容生态安全风险治理的合理性和有效性：

（1）整体智治强调对网络信息内容生态安全风险的多主体、多维度、多要素、多机制的治理。这种整体性理论框架的建构不是简单地将某个网络服务平台、某个网络社区或某些主题或事件领域的内容安全危害事件等同于网络信息内容生态安全风险。"内容安全风险"既可能演化为不良或违规信息内容传播的危机或危害事件，也可能通过对有关风险源的识别与预警，

提示各方参与主体通过多种正面信息投放机制和主动的对向标示治理与价值观引导，将内容生态安全风险进行分散、转移和消除等。整体智治理论框架的构建可以为“内容聚集样貌”的整体性转变和良好生态状态维护提供系统性理念与方法指导。

（2）整体智治强调对内容生态安全风险的全流程和智慧性治理。全流程和智慧性要求治理工作必须关注内容安全风险监测预防、研判分析、风险分散与消除和危害性内容安全事件发生后的应对处置等所有环节。从信息生命周期理论和网络信息内容传播演变规律看，网络信息内容的生成、传播、变异、蜕变和消失等也有一个动态演变过程。以往我们对网络信息内容安全风险问题的关注一般是将重点放在安全风险问题明显暴露或安全风险事件发生后的应对处置上，以年度为单位开展“专题”或“专项”的运动式网络治理就是一个例证。整体智治理论框架的全程性和智慧性特征，从流程上揭示了内容安全风险监测与预防、风险研判与分析、风险分散与消除和风险转化了危害性事件后的应对处置之间的内在关系，从实现手段上将信息技术运用放在突出位置。这种全程性和智慧性治理思维将会进一步明确形成以防为主、防治结合的总体工作策略，极大地提高网络信息内容生态安全风险治理的效率与效能。

2.3 网络信息内容生态安全风险整体智治理论框架构建的意义

通过对整体智治理论框架构建逻辑、合理性与有效性及其与已有治理模式运行特征的比较分析，可以认为，整体智治更加重视提升所有治理参与主体的合力、治理资源配置能力、信息技术的中介联接能力和治理行动与目标的规划能力等。整体智治理论框架构建的意义是：

2.3.1 改变现有治理模式构建与运作的问题导向思维，更加突出目标导向思维

政府监管模式、多元共治模式和网络自治模式无论其内部运行机理如何，其一般都是以“问题导向”作为治理的基本原则，这个原则对解决当下已经出现的内容生态安全风险隐患或风险事件无疑具有积极作用，为了实现对网络内容生态安全风险隐患或事件的快速治理，与此相适应的针对特定领域或特定问题而采取的分类/分散治理策略似乎比较受青睐，但它也表征出治理模式的功利主义取向。整体智治的理论框架是以网络信息内容生态安全环境的整体性样貌为治理目标，以信息技术中介来联接整体性与智慧性治理要求，从总体上对我国网络信息内容生态环境特征及其隐藏的风险因素作出趋势分析与预防研判，而不是局限于对某类平台、某类主题等网络信息内容安全风险事件发生后的应对处置。

2.3.2 重视现有治理模式的体制与机制障碍，更加突出整体性治理发展趋势

中国政府的组织结构是条块分割的二维模式[38]。当前，无论是政府监管模式还是以政府为主导的多元共治模式，均强调在网络信息内容治理中政府有关部门的广泛参与，这些部门涉及宣传、政法、公安、工信、新闻出版等多个条线，并辅之以网络信息服务平台属地管理原则。在这种条块体制下，由于部门利益、“专业主义”以及科层体系繁杂的程序和规则，“条”与“条”、“条”与“块”之间的政策壁垒广泛存在，条块之间治理协作非常困难。而网络自治模式则又因相关主体的利益驱动导致网络内容生态安全整体的自组织性受到削弱。以信息技术为中介联接的整体性与智慧性融合治理，一定程度上可以在体制与机制对上述条块障碍和自组织障碍进行突破。

2.3.3 正视既有治理模式的人工依赖及其低效性，更加强调现代信息技术的广泛运用

从实践看，既有 3 种治理模式在运作中往往依赖于大量人力资源投入(例如所谓“网络水军”就有此层含义)，虽也有技术运用，但其运用的广度与深度还比较有限。人工智能技术、大数据技术等在网络信息内容生态安全风险治理实践中已经被证明有广泛应用可能与前景。有专家认为，目前 90% 以上的海量实时多媒体内容都可以被智能技术精准识别过滤，自然语义、图像识别、声纹识别等都在内容安全领域均有成熟彻底的落地方案[39]。在整体智治的理论框架构建中突出信息技术的地位，不仅可以提高内容安全风险识别与治理的效能，而且可以对安全风险演化动态作出趋势性预防，从而体现出主动治理思维。

3 网络信息内容生态安全风险整体智治的实现策略

网络信息内容生态安全风险整体智治理论框架的构建体现出以信息技术为中介联接的整体性与智慧性治理有机融合理念，在其实现上可以进行以下策略设计：

3.1 建立制度化的机制保障体系

以法治为基础而建立的网络信息内容安全风险防

控机制是整体智治理论框架构建的应有之义，规则与制度也是任何一种网络治理模式不可或缺的内容。如何通过制度建设与完善来构建多元主体协同参与的网络信息内容风险防控机制、网络信息内容生产发布的激励与禁止互补机制、网络信息内容安全风险的多重审查机制、网络信息内容安全风险的归责与救济机制等是机制保障体系建设的核心内容[35]。

3.2 实施智能化的技术支撑体系

在理论上看，大数据等相关技术应用可以实现对网络信息内容安全风险源、风险因素、风险趋势等进行科学分析预测。网络信息内容生态安全风险事件智能预测技术包括图像识别技术、数字水印技术、文本过滤技术、数据获取技术、协议分析技术、数据还原技术、内容分析与过滤技术、深度学习与智能处理技术等。由于相关技术在其他学科均有较好的研究进展，因此如何吸纳并融合相关技术在网络信息内容安全风险规制上的应用就是一个现实的组织操作问题。

3.3 落实生态化的平台治理体系

在我国网络信息内容生态安全治理上坚持的是“政府管平台”“平台管用户”的思路。因资源与技术所限，政府本身并不具备对网络信息内容生态安全风险进行全方位治理的能力，因此在制度上突出了让网络信息内容服务平台承担更多义务与责任的安排。如何形成并完善服务平台内部的内容生态安全治理体系就十分关键，主要途径是：通过过程管理制度的构建，从健全用户注册、账号管理、信息发布审核、跟帖评论审核、版面页面生态管理、实时巡查、应急处置和网络谣言、黑色产业链信息处置等方面进行风险关节点的管理，从而保障网络信息服务平台本身就是一个良好的内容生态系统；从账号注册、登录、用户行为、内容发布以及登出等过程，构建一个全链路的内容安全风险控制体系，运用多种技术对用户进行画像并实施对用户全生命周期的管理；通过完善平台系统内部的规则体系来满足治理要求。这些规则通常是以“用户协议”“行为规范”等形式出现，用户必须同意相关规则才能顺利注册账户。这些内部规则虽反映了网络法律法规与网络规范的要求，但也较多体现了平台自身的利益与需求。

3.4 构建系统性的内容生产投放体系

内容生态安全风险整体智治的理论框架突出了正负面信息的对向标示治理，这意味着在治理行动中不仅有负面信息的被动清理与删除，而且有正面信息的主动生产投放。能动性的内容生产投放体系就是要通过主动的话语构建来实现对舆论场的主导。“话语”始终与社会制度和社会实践联系在一起，“话语”结构是一套固有的规则，它决定着认识行为的形式与内容，同时也决定着网络信息内容是否存在安全风险。不同类型的网民依据“固有的规则”，将其“话语”传播到网络空间之中，这就可能会因其规则的不同而引发安全风险。在用户生产内容成为一种常态后，政府机关及有关内容生产部门能否积极主动地开展内容生产投放并进一步增强投放力度等就决定着内容生态安全风险能否得到主动防控。因此，官方主流媒体、用户集聚度高的社交媒体平台应主动担当起正能量导向的内容产品生产与投放责任，政府有关部门也可以主动对网络内容主题进行系统策划，对有关社交媒体的内容生产投放状态进行定期评价，并实施相关激励与惩罚措施。

3.5 建立常态化的归档保存体系

网络信息内容的流失风险是其内容生态安全风险中较少被引起关注的侧面。虽然近年来有学者对网络信息归档保存进行了研究，但并未将其放在网络信息内容安全风险规制的视角来对待，国内有关网络信息内容常态化归档保存的制度和机制尚未形成。立足事件、主题等维度进行网络信息内容的全景调查并及时进行选择性归档保存，有利于形成确保重大社会事件、重大议题得以被识别，更真实完整地还原事件、议题演变趋势本身，从而形成较完整的社会记忆资产。这种网络信息内容安全风险规制具有保证数据资产安全和国家记忆安全的意义。

4 总结与讨论

综上所述，网络信息内容生态安全风险整体智治理论框架，有着其独到的内在意涵和构建逻辑，即其治理指向对象是内容生态安全风险的整体样貌，发动治理的动力是实现良好的内容生态环境目标而不是某类具体的风险问题或事件，它重视行动者、技术工具和规则体系之间的协同关系，突出了信息技术的中介作用，体现出整体性与智慧性治理融合等逻辑特征。由于篇幅所限和当前治理案例仍是以“周期性主题类专项行动”“定点定向类专项行动”“大内容服务平台针对类行动”以及“突发应急类专项行动”等治理行动为主，尚未体现出整体智治的理念和框架要求，因此，在现阶段尚无法通过具体案例来有效验证这个理论框架的科学性和实效性，这也是目前本文研究的局限所在。在后续研究中，笔者将会注意通过对一些已有实践案例中的“反例”数据或样本采集，来进一步验证整体智治理论框

架的必要性、合理性和实现策略的可行性,并通过具体实现路径设计来推动理论框架和实现策略的具体落地。

参考文献:

[1] CARAVELLI J, JONES N. Cyber security: threats and responses for government and business[M]. California: ABC-CLIO,2019.
[2] 何明升. 网络内容治理的概念构建和形态细分[J]. 浙江社会科学,2020(9):64－72.
[3] 赵蓉英,余波. 网络信息安全研究进展与问题探析[J]. 现代情报,2018,38(11):116－122.
[4] 李源粒. 网络数据安全与公民个人信息保护的刑法完善[J]. 中国政法大学学报,2015(4):64－78, 159.
[5] 支振锋. 网络安全风险与互联网内容治理的法治化[J]. 改革,2018(1):44－46.
[6] 何明升. 中国网络治理的定位与现实路径[J]. 中国社会科学,2016(7):112－119.
[7] 周毅. 数字遗产保存的行动路线研究[J]. 情报理论与实践,2012,35(4):15－20.
[8] 支振锋. 提升网络生态治理效能的制度探索[J]. 信息安全与通信保密,2020(2):5－11.
[9] 周毅,吉顺权. 网络空间多元主体协同治理模式构建研究[J]. 电子政务,2016(7):2－11.
[10] 谢新洲,李佳伦. 中国互联网内容管理宏观政策与基本制度发展简史[J]. 信息资源管理学报,2019(3):41－53.
[11] 王平. 多元视角下用户生成内容的信息质量评估研究[M]. 北京:科学出版社,2020.
[12] 朱庆华. 新一代互联网环境下用户生成内容的研究与应用[M]. 北京:科学出版社,2014.
[13] 苏新宁. 应急响应情报体系:理论、技术与实践[M]. 北京:科学出版社,2019.
[14] 王世伟. 论信息安全、网络安全与网络空间安全[J]. 中国图书馆学报,2015,41(3):72－81.
[15] KIMANI K, ODUOL V, LANGAT K. Cyber security challenges for IoT-based smart grid networks[J]. International journal of critical infrastructure protection, 2019, 25(1):36－49.
[16] 马费成,李小宇. 中国互联网内容监管主体结构与演化研究[J]. 情报学报,2014,33(5):452－464.
[17] 黄如花,温芳芳. 在开放政府数据条件下如何规范政府数据:从国际开放定义和开放政府数据原则谈起[J]. 情报理论与实践,2018,41(9):37－44.
[18] 何明升. 网络内容治理:基于负面清单的信息质量监管[J]. 新视野,2018(4):108－114.
[19] PROVAN K G, KENIS P. Modes of network governance: structure, management, and effectiveness[J]. Journal of public administration research and theory, 2008, 18(2): 229－252.
[20] HÜTTEN M. The soft spot of hard code: blockchain technology, network governance and pitfalls of technological utopianism[J]. Global networks, 2019, 19(3): 329－348.
[21] 马费成,李小宇. 中国互联网内容监管主体结构与演化研究[J]. 情报学报,2014,33(5):452－464.
[22] DAVIS R E. Auditing information and cyber security governance[M]. Los Angeles: CRC Press,2021.
[23] PARDINI D J, HEINISCH A, PARREIRAS F S. Cyber security governance and management for smart grids in Brazilian energy Utilities[J]. Journal of information systems and technology management,2017,14(3):385－400.
[24] 许鑫. 西方国家网络治理经验及对我国的启示[J]. 电子政务,2018(12):45－53.
[25] QIAN X M, ZHANG J Y. Global cyber security governance in the new era: status, dilemma, and development[C]//2020 International conference on materials, control, automation and electrical engineering. Piscataway: IEEE Press,2020:41－45.
[26] 周毅. 试论网络信息内容治理主体构成及其行动转型[J]. 电子政务,2020(12):41－51.
[27] LARSSON O L. The governmentality of network governance: collaboration as a new facet of the liberal art of governing[J]. Constellations, 2019, 27(1): 111－126.
[28] 郁建兴,黄飚. 整体智治:公共治理创新与信息技术革命互动融合[N]. 光明日报,2020－06－12(11).
[29] 朱浩齐. 构建全链路内容风控体系解决内容安全难题[J]. 中国信息安全,2020(2):73－74.
[30] PERRI 6, DIANA L, KIMBERLY S, et al. Towards holistic governance: the new reform agenda[M]. New York: Palgrave, 2002.
[31] 谭成华. 智慧治理的内涵、逻辑和基础分析[J]. 领导科学,2019(12):51－54.
[32] 陈成文. 论市域社会治理的风险防控能力[J]. 社会科学家,2020(8): 15－20.
[33] 朱勤. 技术中介理论:一种现象学的技术伦理学思路[J]. 科学技术哲学研究,2010(1):101－106.
[34] 王丛. 新闻自动生成——人工智能正在逐步走进金融领域[EB/OL]. [2021－10－21]. http://blog.memect.cn/? p=75.
[35] 周毅. 论网络信息内容生态治理机制的构建[J]. 情报杂志,2020,36(12):96－101.
[36] 陈堂发. 网络公共性表达法治问题研究[M]. 广州:中山大学出版社. 2017.
[37] WANG T, ULMER J R, KANNAN K. The textual contents of media reports of information security breaches and profitable short-term investment opportunities[J]. Journal of organizational computing and electronic commerce, 2013, 23 (3):200－223.
[38] 余敏江. 整体智治:块数据驱动的新型社会治理模式[J]. 行政论坛,2020(4):76－82.
[39] 朱浩齐. 构建全链路内容风控体系解决内容安全难题[J]. 中国信息安全,2020(2):73－74.

作者贡献说明:

周毅:论文思路提出,论文写作与修改定稿;
张雪:论文资料收集整理,部分内容修改等。

Research on the Theoretical Framework and Realization Strategy of the Holistic Intelligent Governance for the Ecological Security Risk of Network Information Content

Zhou Yi Zhang Xue
School of Sociology, Soochow University, Suzhou 215123
Center for Data Governance and Industrial Development, Soochow University, Suzhou 215123

Abstract: [Purpose/significance] The ecological security risk of network information content is a new type of information ecological security problem, which affects and threatens the overall national security from multiple dimensions. [Method/process] Based on the theory of holistic governance, intelligent governance and technological intermediation, this paper put forward the concepts, logical relations and basic contents of the theoretical framework construction of holistic intelligent governance of network information content ecological security risk, and specifically explained the significance of the theoretical framework construction of holistic intelligent governance. [Result/conclusion] The paper signifies the theoretical framework construction of holistic intelligent governance of network information content ecological security risk is an organic fusion of integrity and intelligent governance with information technology as the intermediary. In order to specifically promote its organization and implementation, the implementation path can be selected from the construction of an institutionalized mechanism guarantee system and the implementation of an intelligent technical support system.

Keywords: ecological security risks of network information content holistic intelligent governance theoretical framework realization path